# PANOS APIs

*April 2011*

*Marc Benoit*

paloalto NETWORKS

paloalto NETWORKS

the network security company™

paloalto NETWORKS

API, an abbreviation of ***A****pplication* ***P****rogramming* ***I****nterface*, is a set of routines, protocols and tools for building software applications.

Good API's should provide all the building blocks required for a programmer to assemble them into useful applications (….including documentation!)


© 2011 Palo Alto Networks. Proprietary and Confidential.

SE's face a myriad of technical sales objections during sales cycle

API's can be leveraged to solve complex integration questions

Be aware of what is available and what is coming…

Don't be afraid to demonstrate API's

- You DON'T need to be a programmer or an expert
- You DO need to be able to leverage tools and be familiar with concepts

API's can help you close deals

- Sell around objections
  - Usually just demonstrating our API's puts prospects at ease regarding integration
  - Other vendors have been promising flexible API's for years and haven't delivered
    - Clear differentiator
- Don't paint yourself into a corner
  - Don't volunteer to write scripts or solve all of a prospects problems!


© 2011 Palo Alto Networks. Proprietary and Confidential.

REST API

External system can manage device from remote

Can show/set/edit/delete the device config

Can poll ACC/Pre-defined/Custom report from the device

User-ID API

User-ID integration with external system

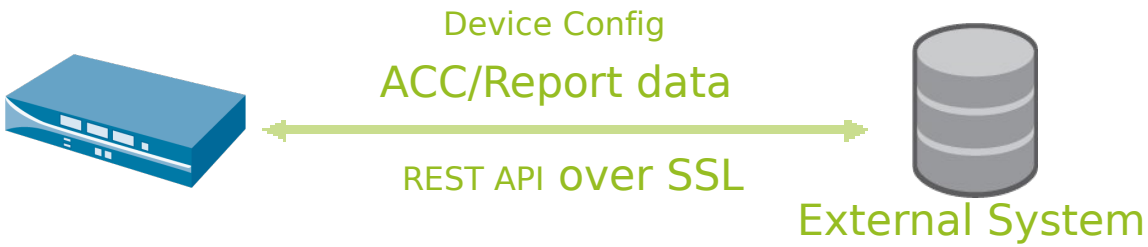
Can add/delete ip-username mapping info against UIA

External system can connect to the device mgmt interface over SSL

External system can use REST API to see/change device config AND/OR get report data in XML format

API  communication requires a key generated with admin ID and password info

SSL connection from external system is treated as general admin web access, so same source address restriction and timeout setting would be applied



- Step 1 : generate Key for API communication

Key  generation request example:
https://hostname/esp/restapi.esp?type=keygen&user=username&password=password

Key generation response example:

```
<response status="success">
    <result>
        <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
    </result>
</response>
```

- Step 2 : specify the *type* [*config* | *report*]

- *type = config  (NOTE: REQUIRES SU ACCESS!)*
  - Specify the *action*  [*show* | *set* | *edit* | *delete*]
  - Set each config item in *xpath*

*Xpath*  example

xpath=devices/entry/vsys/entry/rulebase/security

Example: Get security rulebase info from device config

https://hostname/esp/restapi.esp?type=config&action=show&key=keyvalue&xpath=devices/entry/vsys/entry/rulebase/security

Example: Add config to device

https://hostname/esp/restapi.esp?type=config&action=set&key=keyvalue&xpath=xpath-value&element=element-value

- *type = report*
  - Specify the *reporttype* [*dynamic* | *predefined* | *custom* ]
  - Specify *reportname*
  - Can specify the *period* OR *starttime* & *endtime* *optional

Example : Get Application Top 5 data from ACC

https://hostname/esp/restapi.esp?type=report&reporttype=dynamic&reportname=top-app-summary&period=last-hour&topn=5&key=keyvalue

Example : Get the “top-attackers-summary” data from pre-defined report

https://hostname/esp/restapi.esp?type=report&reporttype=predefined&reportname=top-attackers-summary&key=keyvalue

How can I demonstrate the API?

Leverage simple examples in a web browser

***Get a key:***

https://10.xx.10.50/esp/restapi.esp?type=keygen&user=admin&password=admin

***Backup your config:***

https://10.xx.10.50/esp/restapi.esp?type=config&action=show&key=0RgWc42Oi0vDx2WRUIUM6A=

***Generate a report:***

https://10.xx.10.50/esp/restapi.esp?type=report&reporttype=dynamic&reportname=top-app-summary&period=last-hour&topn=5&key=0RgWc42Oi0vDx2WRUIUM6A=

***Don't sell past the close…..***


© 2011 Palo Alto Networks. Proprietary and Confidential.

External system uses SSL/TLS to connect to User-ID Agent

External system can send user login/logout event info to Agent in XML

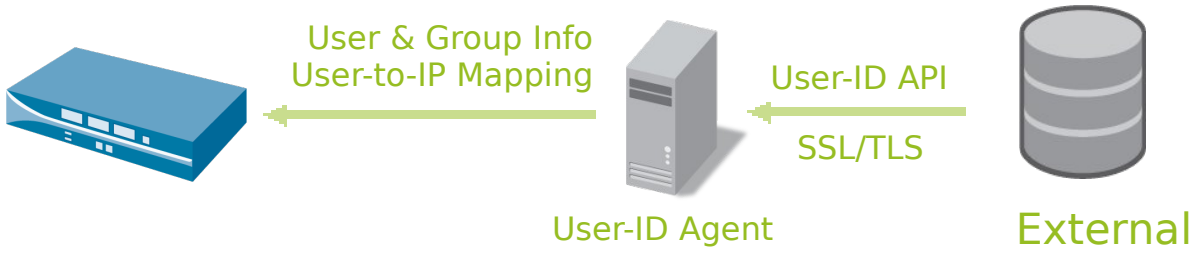
Agent  sends response back in XML

External system can keep connection up to send continuous data OR it can close the connection as necessary

Each User-ID Agent can have up to 100 connections simultaneously

If there's no traffic for 10min, Agent would close the connection automatically

To keep connection up, external system can send keepalive packet



```
<uid-message>
   <version>1.0</version>
<type>update</type>
   <payload>
      <login>
         <entry name=”domain\uid1” ip=”10.1.1.1”>
         <entry name=”domain\uid2” ip=”10.1.1.2”>
         <entry name=”domain\uid3” ip=”10.1.1.3”>
      </login>
      <logout>
         <entry name=”domain\uid4” ip=”10.1.1.4”>
      </logout>
</payload>
</uid-message>
```

# Leverage what already exists

# MAC logon script pack

- Contains PAN::API.pm

New version on the way with error checking etc from Martin

Great example program for how to interact with User-ID API

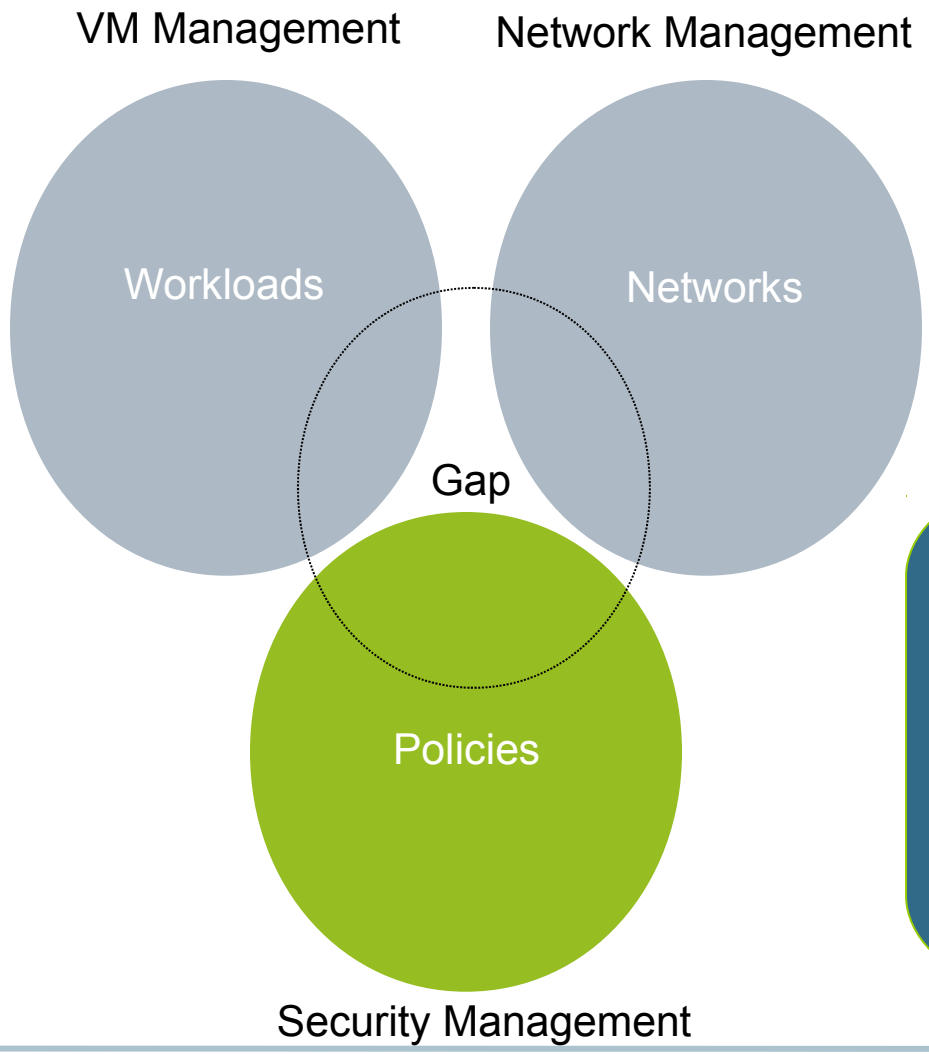
Some additional samples…..

VB scripts for windows logon script can be leveraged (Nick P)

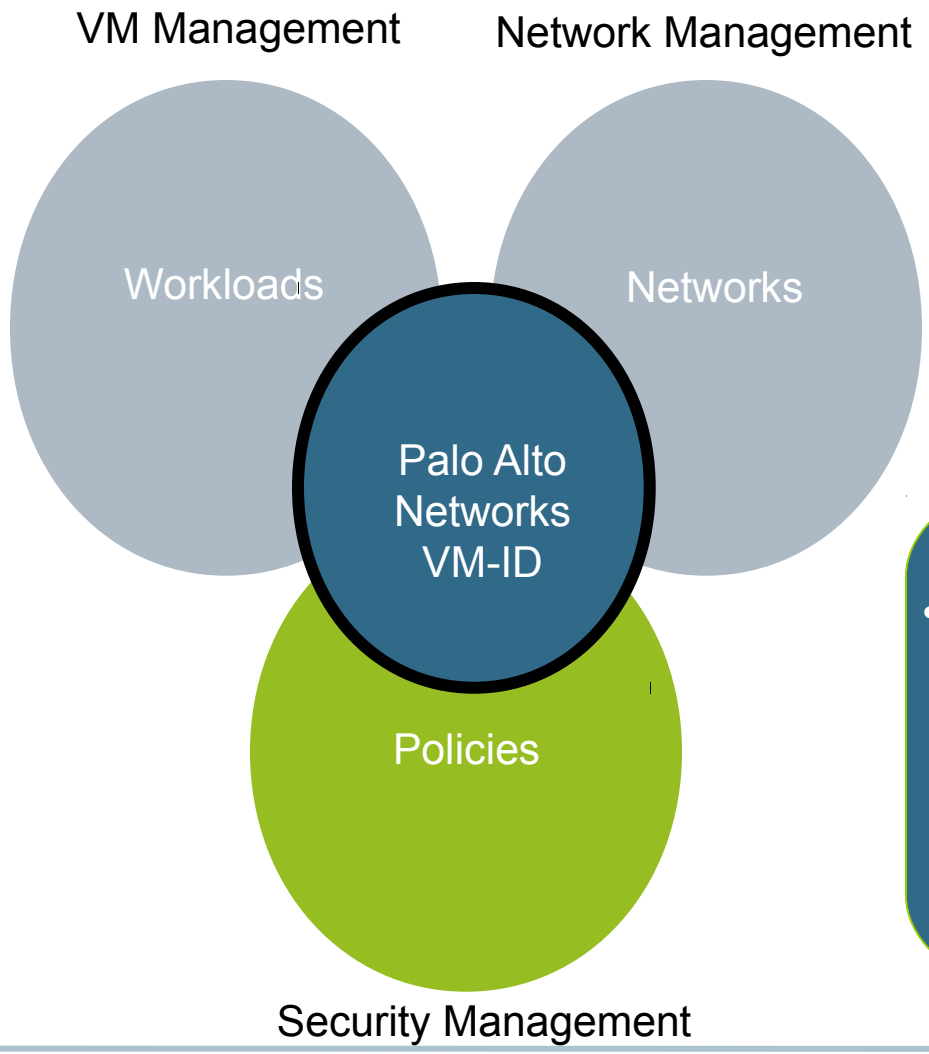
VMWare integration for visibility


© 2011 Palo Alto Networks. Proprietary and Confidential.

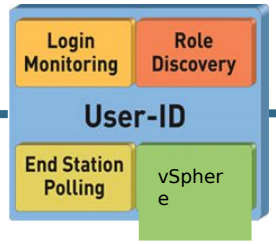
# •User-ID XML API use case: Virtualization Security Visibility

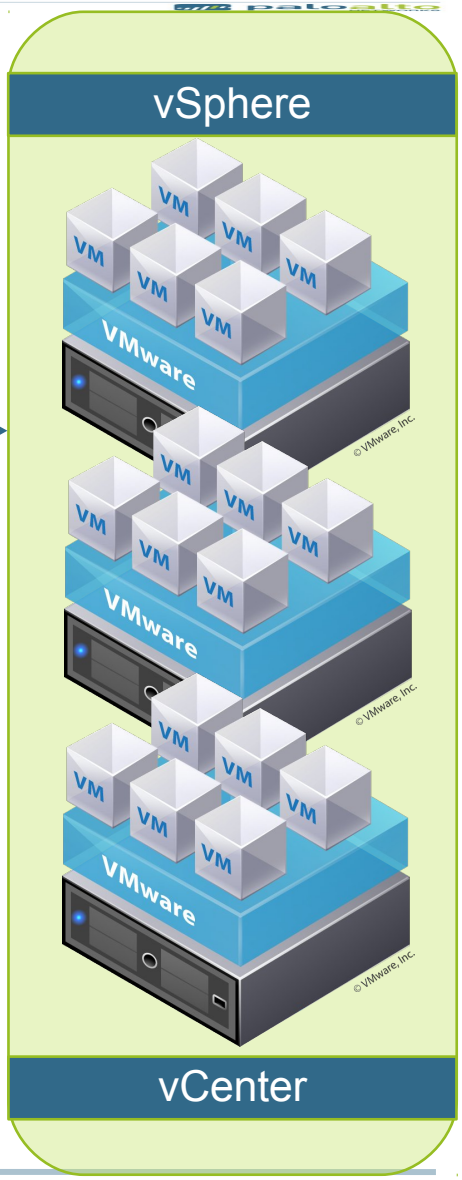



- *No data synchronization*
- *No visibility across functions*
- *Manual, error-prone*




- *Cross-functional visibility & Control*
- *Real-time*
- *Fully automated*




1. User-ID Agent Polls vCenter or ESX(i)
2. Agent Publishes VM Mapping
3. VM Visibility in ACC
4. Dynamic VM Adds/Moves auto-sync

**Top Sources**

| | Source address | Source Host Name | Source User | Bytes | Sessions |
|---|---|---|---|---|---|
| 1 | 10.30.10.101 | 10.30.10.101 | win7-564d47f0-a182-7fc0-2e68-b | 1.2 M | 4.0 K |
| 2 | 10.30.10.102 | 10.30.10.102 | ubuntu-564de08b-8d50-4e3b-cadc | 639.5 K | 2.3 K |
| 3 | 10.30.10.103 | 10.30.10.103 | winxp-564db5c4-703d-c248-25bc- | 463.5 K | 1.4 K |

***Binds VM->IP***

***Report on VM and User->VM Activity***



© 2011 Palo Alto Networks. Proprietary and Confidential.

# •User-ID XML API use case: Palo Alto Networks/Enterasys

the network security company™

User-ID requires directory data for User->Group mapping

User->IP Obtained via passive and active mechanisms

Windows Security Logs

NTLM auth/Captive Portal

WMI Scanning/Open Server Sessions

Point of Entry

Must register devices when entering/exiting the network

XML UID-API available

Mobility (Wired/Wireless)

Must trigger re-map of the user to the new network

Must automatically de-associate the user with prior IP's

Simplify Design – no complex MS integration required



© 2011 Palo Alto Networks. Proprietary and Con[illegible]ntial.

enterasys® Secure Networks™

paloalto NETWORKS

# User->IP mapping is critical for dynamic security policy

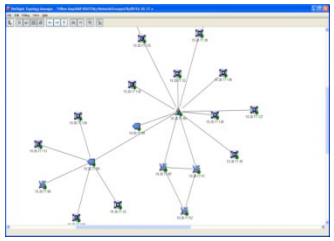
## Mapping mechanisms need to be extended to the actual point of entry on the network

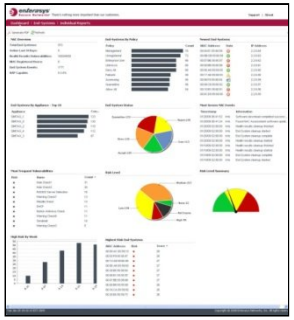
- Wired and Wireless network join/authentication
- If not forcing users to auth, capture unique data (like MAC)
  - Users today have many devices: Laptops/Iphones/Tablets
  - Leading to the Consumerization of IT
    - Trend is becoming difficult to ignore
    - Users expect to use their own devices
    - Users expect little disruption to their usability/experience
    - Corporate Security policy still needs to be maintained

Joint Solution offers granular, accurate mapping of user entry and egress from network

Creates higher accuracy for dynamic policy enforcement and reporting


© 2011 Palo Alto Networks. Proprietary and Confidential.





© 2011 Palo Alto Networks. Proprietary and Confidential.

# •XML API use case: Palo Alto Networks/Enterasys

the network security company™

Leverages XML API to extract application data per user

Publishes additional meta data to Enterasys NAC appliance

They obtain context regarding application usage to leverage when making internal network access decisions

Integration issue: Their unique identifier is MAC address


© 2011 Palo Alto Networks. Proprietary and Confidential.

User->App mapping is critical for posture assessment and security compliance

Palo Alto Networks rich application data adds depth to Enterasys NAC reporting

Critical for Endpoint Compliance/Posture Assessment

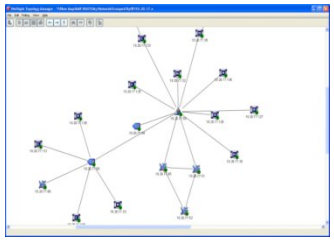
Additional Usage Data for endpoint policy/access control

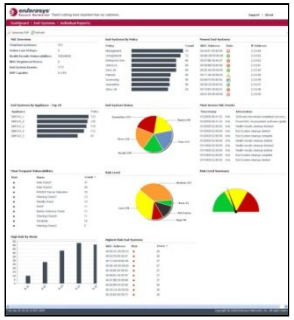
Apply heuristics to determine suspicious endpoints

- Earlier detection of malicious worms, botnet activity

Joint Solution offers unprecedented visibility and control of all enterprise managed and unmanaged assets


© 2011 Palo Alto Networks. Proprietary and Confidential.





© 2011 Palo Alto Networks. Proprietary and Confidential.

# •Community Supported Tools

***Business Development***

the network security company™

Palo Alto Networks offers a rich XML API

Limited documentation and low adoption

Tremendous potential!

Emerging markets like Service Providers often have custom data management requirements

For example, allow customers to have branded, customized and limited interface integrated within their existing customer portal

Automated provisioning of new customers

Current Interfaces offer little customization


© 2011 Palo Alto Networks. Proprietary and Confidential.

# Provide reference implementations

# Simplify XML-API use through convenience libraries

- Like a CLI for the XML API

Scripts and examples of actual integrations

Supported by responsive online community

Distributed under the CC License

The software is provided “as is”

Permission to use, copy, modify, and/or distribute the software free of charge

Partners, resellers & SP/SI’s can modify existing reference implementation and/or build their own from scratch

## Allows partners and customers to easily extend Palo Alto Networks solutions by developing custom tools

## Increases Professional Services $$$ and possible support contracts for integration partners


© 2011 Palo Alto Networks. Proprietary and Confidential.

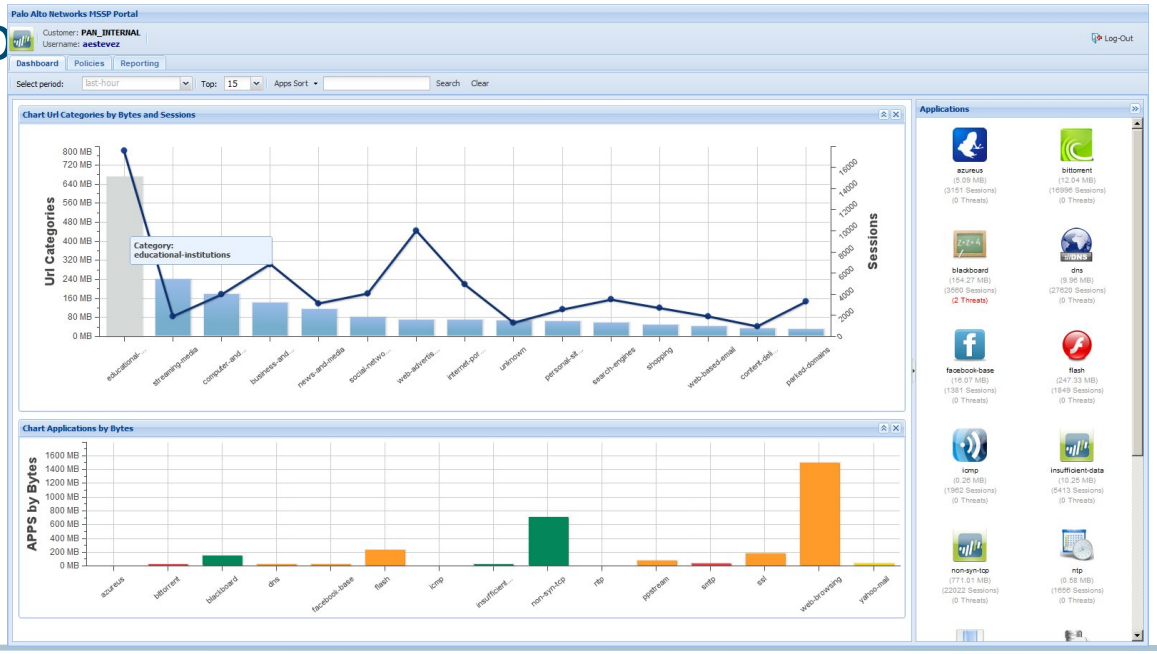
SDK consists of VM and Source Code Package

Includes reference implementation of an MSSP Custom Portal

Utilizes standard LAMP stack (Linux, Apache, MySQL, PHP)

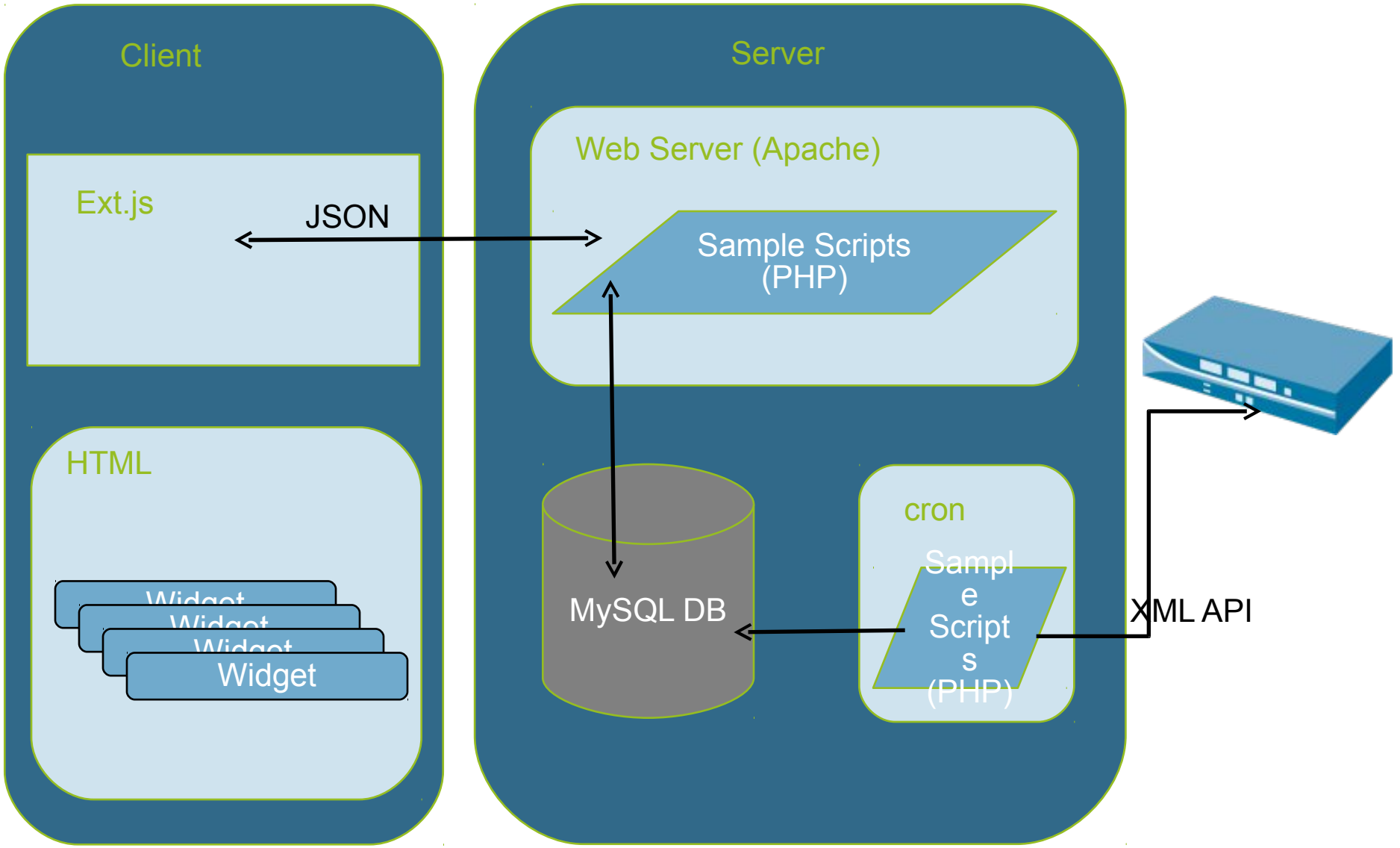
EXT.JS GUI Framework for example presentation layer

PHP Scrip






© 2011 Palo Alto Networks. Proprietary and Confidential.





© 2011 Palo Alto Networks. Proprietary and Confidential.

What it's not……

A Replacement for Panorama

A Replacement for the device GUI

An alternative GUI to address a FR

What does it address?

Environments where significant customization is required

Existing portals that need access/interface to rich data from Palo Alto Network's Firewalls.


© 2011 Palo Alto Networks. Proprietary and Confidential.

## Package consists of Perl XML-API wrapper

## Simplifies interactions with XML-API (command line)

## Provides utility and convenience libraries for common functions

- PCAP export, templating, remote commit operations etc

Template for fully automated provisioning (SP customers)

- Layer 3 vsys templates for single command automation

Many Utility functions

- Backup FW's/Panorama using XML API or CLI Expect
- Threat PCAP path identification (EPOCH Time converter) and Export tools
  - Perl daemon for exporting/archiving all pcaps
- Use to migrate objects/policies from Device to Panorama
- Simple way to demonstrate XML API functionality and flexibility

Ongoing development to add functions and capabilities


© 2011 Palo Alto Networks. Proprietary and Confidential.

## An online community of Palo Alto Networks Next Generation Firewall Users

Customers

Resellers and partners

Palo Alto Networks System Engineers and Professional Services

Palo Alto Networks Tech support

Other technical experts within the company

## Exchange of ideas on how to develop, deploy and support customized, web-based applications

Forum

File sharing

Documentation


© 2011 Palo Alto Networks. Proprietary and Confidential.

Online Community for customers, partners, employees to share and discuss custom content at:

https://live.paloaltonetworks.com/community/devcenter

What custom content?

Custom App-IDs; Custom Threats; CLI Scripts; API integration; More…

Need support?

Use discussion threads to ask questions and discuss

Members (SE, Customer, Partner, PM) offer & receive help from others

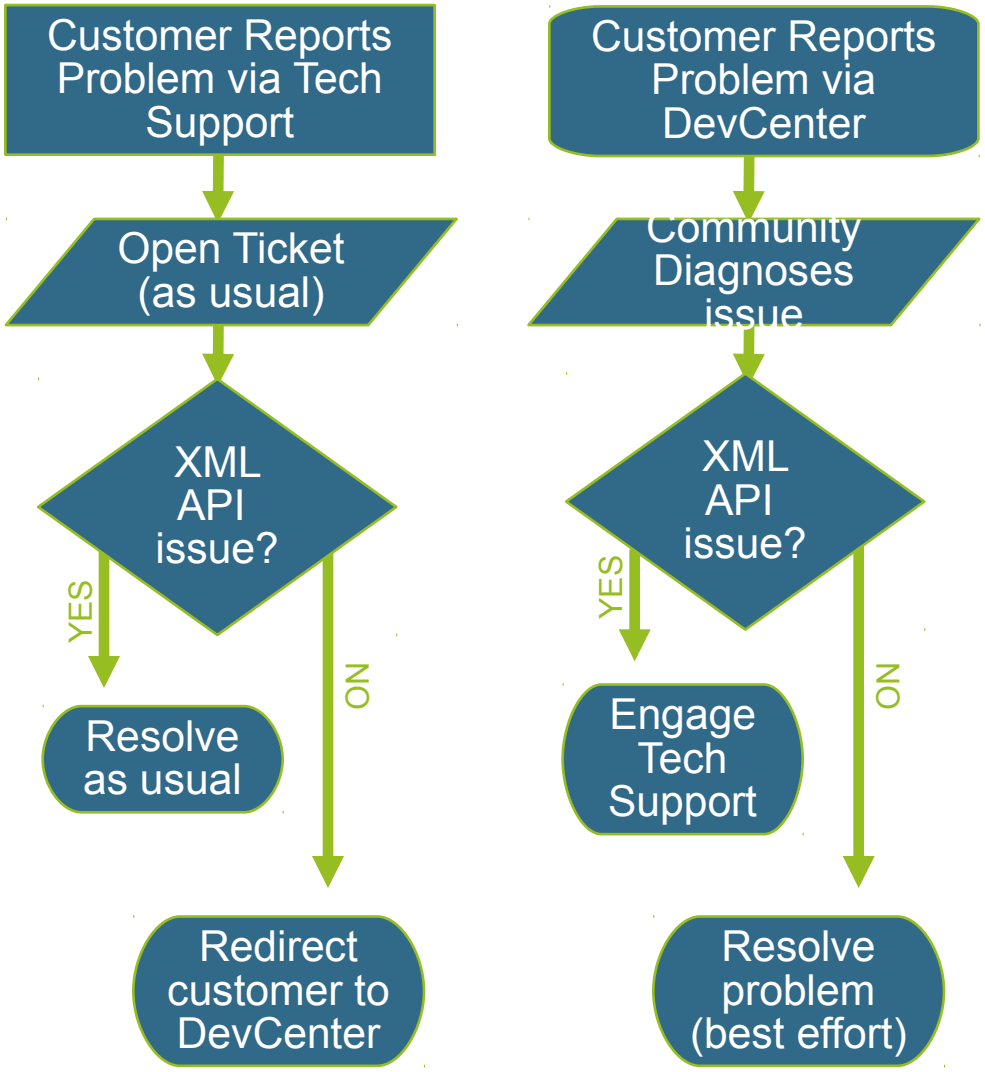
PM team offers documentation, guidelines, samples, etc.

Support team will focus on software features but not specific signatures/scripts made available on DevCenter

Licensing for posted content

Click to edit Master text styles
Second level
Third level
Fourth level
Fifth level
paloalto NETWORKS
Next Generation Enterprise Firewalls
PRODUCTS
SOLUTIONS
INFO CENTER
SUPPORT
PARTNERS
NEWS & EVENTS
COMPANY
CONTACT
Live Community
Welcome, mbenoit (Log out)
New
Your Stuff
History
Browse
Palo Alto Networks Live > DevCenter
DevCenter
Overview
All Content (70)
Discussions (29)
Documents (40)
Blog
Videos
Set as default tab
Welcome to DevCenter!
The online community for customers, partners, and employees to share custom content including Custom App-IDs, Custom Threats, Custom Reports, XML API integration, CLI scripts, and other tools. Use the discussion threads to ask questions and receive help from other members. The current samples would be a good start. Have fun!
Recent Discussions
GlobalProtect - Force client connection
1 day ago
by firewall@idealnetsrl.it
Re: Retrieve apps using XML API
2 weeks ago
by robbrooks70
White list issue
2 weeks ago
by sdmcglocklin
Teamviewer sub-applications better recognition
3 weeks ago
by lardsa
Re: How to REJECT instead of DROP?
3 weeks ago
by lardsa
More
License
Content on DevCenter is made available with the hope that it will be useful, but without any warranty. All content is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. By posting content here, you agree to license it under the same license.
Actions
Start a discussion
Create a document
Create a video
Write a blog post
Notifications
Stop email notifications
Stop following this community
View feeds


© 2011 Palo Alto Networks. Proprietary and Confidential.




## XML API is part of the product

Customers are entitled to Palo Alto Networks technical support for the XML API

## The DevCenter Community is the official SDK/tools support infrastructure

Best-effort level of support

Goal of community is to be very responsive – SLA?


© 2011 Palo Alto Networks. Proprietary and Confidential.

## Other vendors provide an API too

- CheckPoint (OPSEC)
- Juniper (XML)
- Fortinet (XML)

## Only Palo Alto Networks provides integration examples

- Automated Provisioning (PAN-Perl)
- Customizable Interface (WebService SDK)
- Examples provides high-level API abstraction and error handling
- Advanced JavaScript toolkit (web 2.0) for front-end features
- Free, online community support


© 2011 Palo Alto Networks. Proprietary and Confidential.

## Support for Operational Commands

Setting, Showing, Clearing runtime parameters

Saving and loading configuration to/from disk

Requesting system level operations…e.g.  Content upgrade

Schedule jobs

## Support for additional Configuration Commands

GET, RENAME, MOVE, etc.

## Support for Commit

## Support for Packet Capture (PCAP) Exports

## URI Change

`NEW: https://hostname/api/?query`

`OLD: https://hostname/esp/restapi.esp?query (backward compatible)`

`API Browser: https://hostname/api`

Click to edit Master text styles

Second level

- Third level
  - Fourth level
    - Fifth level

Home > config > devices > vsys > rulebase

application-override
captive-portal
decryption
dos
nat
pbf
qos
security

**XPath**

```
/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase
```

**XML**

```
<config><devices><entry name='localhost.localdomain'><vsys><entry
name='vsys1'><rulebase></rulebase></entry></vsys></entry></devices></config>
```

**Rest API Url**

/php/rest/api.php?type=config&action=get&xpath=/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase

# •Demo

paloalto
NETWORKS
the network security company™